

Industrial Cellular VPN Router NR300 User Manual



Guangzhou Navigateworx Technologies Co, Ltd www.navigateworx.com

ogo are the

REVISION HISTORY

Revision	Date	Firmware version	Revision Details
0	Oct 2019	1.0.0(337913f)	Initial release.
1	Dec 2019		Change home page layout of UM, add 1- to-1 NAT

Trademarks and copyright

Guangzhou Navigateworx Technologies Co, Ltd and

trademarks or registered trademarks in China mainland, HongKong and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

NavigateWorx

@2018 Navigateworx Technologies. All Rights Reserved.

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Navigateworx Technologies.

Navigateworx Technologies provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Navigateworx Technologies may make improvements and/or changes in this manual, or in the product(s) and/or the program(s) described in this manual at any time.

Information provided in this manual is intended to be accurate and reliable. However, Navigateworx Technologies assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

Technical Support

E-mail: support@navigateworx.com info@navigateworx.com Web: www.navigateworx.com

Interference Issues

Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action, or both.
- Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved or authorized.
- Do not operate in locations where medical equipment that the device could interfere with may be in use.
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.
- Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers.
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers.

Declaration of Conformity

NR300 Series products are in conformity with the essential requirements and other relevant provisions of the CE and RoHS.



Table of Contents

Chapter 1.	Product Overview	5
1.1	Overview	5
1.2	Features and Benefits	5
1.3	General Specifications	6
1.4	Mechanical Specifications	8
1.5	Package Checklist	9
1.6	Order Information	
Chapter 2.	Installation	
2.1	Product Overview	
2.2	LED Indicators	
2.3	Ethernet Port Indicator	14
2.4	PIN Definition of Terminal block	14
2.5	Reset Button	
2.6	Insert SIM card	15
2.7	Install Antenna	
2.8	DIN-rail Mounting	
2.9	Power Supply Installation	
2.10	Power On The Router	
Chapter 3.	Access to Web page	
3.1	PC Configuration	
3.2	Factory Default Settings	
3.3	Login to Web Page	20
Chapter 4.	Web Configuration	21
4.1	Web Interface	21
4.2	Overview	23
4.2.1	Status	23
4.2.2	Syslog	25
4.3	Link Management	26
4.3.1	Connection Manager	26
4.3.2	Cellular	29
4.3.3	Ethernet	
4.4	Industrial Interface	
4.4.1	Serial	
4.5	Network	41
4.5.1	Firewall	41
4.5.2	Route	44
4.5.3	IP Passthrough	45
4.6	Applications	46
4.6.1	DDNS	
4.6.2	SMS	
4.6.3	Schedule Reboot	
4.7	VPN	

4.7.1	OpenVPN	49	
4.7.2	IPSec	54	
4.7.3	GRE	57	
4.8	Maintenance	58	
4.8.1	Upgrade	58	
4.8.2	Software	59	
4.8.3	System	60	
4.8.4	Configuration	64	
4.8.5	Debug Tools	64	
Appendix /	A -Glossary	66	
Appendix I	3 -Q&A	67	
Nc	Signal	67	
Сс	innot detect SIM card	67	
Ро	or Signal	67	
IPS	ec VPN established, but LAN to LAN cannot communicate	68	
Fo	Forget Router Password		
Appendix [- - CLI	69	

Chapter 1. Product Overview

1.1 Overview

Navigateworx NR300 series industrial cellular VPN router offers a single, flexible platform to address a variety of wireless communications needs with over-the-air configuration and system monitoring for optimal connectivity. This router enables wireless data connectivity over public and private LTE cellular networks at 4G speeds.

NR300 series router has dual SIM backup, 1 LAN ports. RS232 and RS485 interfaces are provided to support Serial to IP communication.

NR300 series router supports 9 to 36 VDC wide range power inputs, designed with reverse-voltage protection mechanism for greater reliability. It is an advanced choice for universal wireless M2M applications with reliable features for data transmission.

1.2 Features and Benefits

Industrial internet access

- Wireless Mobile Broadband 2G / 3G / 4G Connection
- Remote access to SCADA System for Industrial Automation
- Reduce high costs for on-site maintenance

Designed for industrial usage

- Power Input Range 9 to 36 VDC
- Industrial designed for harsh environment
- Aluminum casing

Secure and reliable remote connection

- Connection manager ensure seamless communication
- Support Multiple VPN tunnels for data encryption
- Firewall prevents unsafe and unauthorized access

Easy to use and easy maintenance

- User-friendly web interface for human interaction
- Easy configuration for deployment
- Support Central Management Platform

1.3 General Specifications

Cellular Interface

- Standards: FDD-LTE, WCDMA/UMTS/HSPA/HSPA+/EDGE/GPRS,
- 2× SMA female antenna connector
- 2 x SIM (3.0V & 1.8V)

Ethernet Interface

- Standard: IEEE 802.3, IEEE 802.3u
- Number of Ports:
 - 1 LAN x 10/100 Mbps, RJ45 connector
- 1.5KV magnetic isolation protection

Serial Interface

- 1×RS232 (3 PIN): TX, RX, GND
- 1 x RS485 (2 PIN): Data+(A), Data-(B)
- Baud rate: 300 bps to 115200 bps
- Connector: terminal block
- 15KV ESD protection

Other Interfaces

- 1 × RST button
- LED instruction: 1 x SYS, 1 x NET, 1 x USR, 3 x RSSI

Software

- Network protocols: DHCP, ICMP, HTTP, HTTPS, DNS, NTP...
- VPN: IPSec, GRE, OpenVPN, DMVPN, L2TP, PPTP
- Policy: RIPv1/RIPv2/OSPF/BGP dynamic route (optional)
- Firewall & Filter: Port forwarding, DMZ, anti-DoS, ACL
- Serial port: TCP server and client, UDP
- Management: Web, Central Management Platform

Power Supply and Consumption

- Connector: 7-pin 3.5 mm female socket
- Input voltage range: 9~36VDC

• Power consumption:

Idle: 50 mA@12V

Data link: 200 mA (peak) @12V

Physical Specification

- Ingress Protection: IP30
- Housing & Weight: Metal, 200g
- Dimension: 82.8mm x 93.3mm x 28.8mm (excluding antenna)
- Installations: Din-rail mounting

Environmental

- Operation temperature: -40~+75°C
- Store temperature: -40~+85°C
- Operation humidity: 5% to 95% non-condensing

1.4 Mechanical Specifications

Dimension: 82.8mm x 93.3mm x 28.8mm



1.5 Package Checklist

NR300 series Router includes the parts shown in below, please verify your components.

NOTE: if any of the below items is missing or damaged, please contact your sales representative.

Included equipment

• 1 x Navigateworx NR300 series Industrial Cellular VPN router



• 1 x 7-pin 3.5 mm male terminal block for Power Input/RS232/RS485



• 1 x Ethernet cable



• 1 x Quick Start Guide



Optional Accessories (sold separately)

• 3G/4G cellular antenna

Stubby antenna

Magnet antenna





• 35mm Din-rail mounting kit



• AC/DC power adapter (12VDC, 1.5A; EU/US/UK/AU plug optional)



1.6 Order Information

Model	Part Number	Description
NR300-4G	A301430	4G LTE, Dual SIMs, 1 x Eth, 1 x RS232 (3 PIN), 1 x RS485, 9 - 36VDC.

Chapter 2. Installation

2.1 Product Overview

• Front Panel



- 1) Cellular Antenna
- RST Button
 - 3 LED Indicator
 - ④ SIM Slot
 - (5) Power Input/RS232/RS485
 - 6 Ethernet Port



2.2 LED Indicators

Name	Color	Status	Description
SYS	Green	Slow Blinking (500ms duration)	Operating normally
		Fast Blinking	System initialing
		Off	Power is off
		On	Register to Highest priority network
			service (depend on Radio, e.g.
			Radio support LTE as Highest priority
			network).
	Croon	Fast Blinking (500ms duration)	Register to Non-Highest priority
NET	Green		network service (depend on Radio,
			e.g. Radio support LTE as Highest
			priority network, then WCDMA and
			GPRS is non-highest priority network).
		Off	Register failed
		On	Router is trying cellular connection
	Green		with SIM1
		Fast Blinking (250ms duration)	Router is trying cellular connection
			with SIM2
USR: SIM		Off	No SIM detected
		Blinking	Wi-Fi is enabled and data
			transmission
		Off	Wi-Fi is disable or initialize failed
Signal Strength		On, 3 LED light up	Signal strength (21-31) is high
Indicator	Green	On, 2 LED light up	Signal strength (11-20) is medium
T-11	GIEGH	On, 1 LED light up	Signal strength (1-10) is low
¥		Off	No signal

2.3 Ethernet Port Indicator

Name	Status	Description
	On	Connection is established
Link indicator	Blinking	Data is being transmitted
	Off	Connection is not established

2.4 PIN Definition of Terminal block

• Power Input & Serial Port

03	VIN+
01	VIN-
01	GND
01	TXD
01	RXD
01	A
01	B

PIN	RS232	RS485	Power Input	Direction
1			VIN+	Positive (Red Line)
2			VIN-	Negative (Yellow Line)
3	GND			
4	TXD			Router>Device
5	RXD			Router <device< td=""></device<>
6		A		Router<>Device
7		В		Router<>Device

2.5 Reset Button

Function	Action
Reboot	Press the RST button within 3s under operation status
	Press the RST button between 3s to 10s, all LEDs blink few times then
Factory Reset	reboot the router manually.
	Press the RST button more than 10s, router will run normally without
Run Normally	reboot or factory reset.

2.6 Insert SIM card

• Insert / Remove SIM card

- 1. Make sure the power is disconnected.
- 2. Use a Phillips-head screwdriver to remove SIM slot cover.
- 3. Insert the SIM card(s) in to the SIM sockets.
- 4. Replace the SIM slot cover.



2.7 Install Antenna

• Connect the cellular antenna to the MAIN and AUX connector on the unit.



NOTE: NR300 router supports dual antennas with MAIN and AUX connectors. MAIN connector is for data receiving and transmission. AUX connector is for enhancing signal strength, which cannot be used separately.

2.8 DIN-rail Mounting

- 1. Use 4 pcs of M3x6 flat head phillips screws to fix the DIN-rail to the router.
- 2. Insert the upper lip of the DIN-rail into the DIN-rail mounting kit.
- 3. Press the router towards the DIN-rail until it snaps into place.









2.9 Power Supply Installation

- 1. Remove the pluggable connector from the unit, then loosen the screws for the locking flanges as needed.
- 2. Connect the wires of the power supply to the terminals.



2.10 Power On The Router

- 1. Connect one end of the Ethernet cable to the LAN port on the unit and the other end to a LAN port on a PC.
- 2. Connect the AC power to a power source.
- 3. Router is ready when SYS LED is blinking.



Chapter 3. Access to Web page

3.1 PC Configuration

NR300 router contains a DHCP server which will automatically assign an IP address to your PC, however in some cases the user may need to change the network settings on their PC to accept the IP address from the N300. or you can configure a static IP address manually.

• Obtain an IP address automatically

The process required to do this differs depending on the version of Windows you are using. **NOTE:** The following steps are based on Windows 7.

e Edit View Tools Advanced Help				
Organize 👻 Disable this network device Diagnose this c	onnection Rename this connection	ction »	₩ - ▼	
VMware Network Adapter VMnet1 VMwa ② 本地连接 Properties	Internet Protocol Version 4 (TCP/I	Pv4) Properties		
Networking Authentication Sharing Connect using:	You can get IP settings assigned a this capability. Otherwise, you ne for the appropriate IP settings.	automatically if your network supp ed to ask your network administra	orts tor	
JMicron PCI Express Gigabit Ethernet Adapter	Obtain an IP address automa	atically		
Configure This connection uses the following items:	 Use the following IP address IP address: Subnet mask: Default gateway: Obtain DNS server address a Use the following DNS server: Preferred DNS server: Alternate DNS server: Validate settings upon exit 	: sutomatically r addresses: Advance	d	
across diverse interconnected networks.		ОКС	ancel	

select Start » Control Panel » Network Connections. Right click Local Area Connection and select Properties to open the configuration dialog box for Local Area Connection. Select Internet Protocol (TCP/IP) and click Properties to open the TCP/IP configuration window. On the General tab, select Obtain an IP address automatically and Obtain DNS server address automatically. Click OK to complete TCP/IP configuration.

• Set to a static IP address

ganize 🔻 🛛 Disable this network device 👘 Diagnose this	connection Rename this conne	ection »	- 🗌 🔞
VMware Network Adapter VMnet1	Internet Protocol Version 4 (TCP/	IPv4) Properties ? S	
本地连接 Properties	General		
Networking Authentication Sharing	You can get ID settings assigned	automatically if your petwork supports	
Connect using:	this capability. Otherwise, you n	eed to ask your network administrator	
IMicron PCI Express Ginabit Ethemet Adapter	for the appropriate IP settings.		
	Obtain an IP address auton	natically	
Configure	Use the following IP addres	s:	
This connection uses the following items:	IP address:	192.168.5.234	
Glient for Microsoft Networks	Subnet mask:	255.255.255.0	
Gos Packet Scheduler	Default gateway:		
File and Printer Sharing for Microsoft Networks			
□ → Internet Protocol Version 6 (TCP/IPv6)	Obtain DNS server address	automatically	
	O Use the following DNS server	er addresses:	
🗹 🔺 Link-Layer Topology Discovery Responder	Preferred DNS server:		
Install Uninstall Properties	Alternate DNS server:		
Description			
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication	Validate settings upon exit	Advanced	
across diverse interconnected networks.			
		OK Cancel	

click "Use the following IP address" to assign a static IP manually within the same subnet of the router.

NOTE: *Default gateway* and *DNS server* is not necessary if PC not routing all traffic go through NR500 router.

3.2 Factory Default Settings

NR300 router supports Web-based configuration interface for management. If this is the first time for you to configure the router, please refer to below default settings.

Username: **admin** Password: **admin** LAN IP Address: **192.168.5.1** DHCP Server: **Enabled**

3.3 Login to Web Page

- 1. Start a Web browser on your PC (Chrome and IE are recommended), enter 192.168.5.1 into the address bar of the web browser.
- 2. Then use the default username and password(admin/admin), to log in to the router.



Chapter 4. Web Configuration

4.1 Web Interface

The N300 router Web interface is divided into two sections. In the left pane is the main navigation menu. On the right is the content area for each page.

	N mr	Login: admin
Navigatev	worx	Reboot Logout
Overview	Status	
► Overview	System Information	
Syslog	Device Model	NR300-4G
Link Management	System Uptime	01:25:30
Industrial Interface	System Time	2019-10-14 18:50:02
Network	RAM Usage	31M Free/16M Shared/64M Total
Applications	Firmware Version	1.0.0 (337913f)
VPN	Kernel Version	4.4.92
Maintenance	Serial Number	19093014300001
	Active Link Information	
	Link Type	WWAN1
	IP Address	10.146.236.12
	Netmask	255.255.248
	Gateway	10.146.236.13
	Primary DNS Server	120.80.80
	Secondary DNS Server	221.5.88.88
	Copyright © 2018 Guangzhou Navigatewo	orx Technologies Co., Ltd. All rights reserved.

NOTE: The navigation menu may contain fewer sections than shown here depending on which options are installed in your unit.

- **Reboot:** reset the router within power disconnect.
- Logout: logout to web authorization page.



- Save: save the configuration on current page.
- Apply: apply the changes on current page immediately.



• **Close:** exit without changing the configuration on current page.

~	laga
-	lose

4.2 Overview

4.2.1 Status

You can view the system information of the router on this page.

Status	
System Information	
Device Model	NR300-4G
System Uptime	01:25:30
System Time	2019-10-14 18:50:02
RAM Usage	31M Free/16M Shared/64M Total
Firmware Version	1.0.0 (337913f)
Kernel Version	4.4.92
Serial Number	19093014300001

System Information

- Device Module Displays the model name of router
- System Uptime Displays the duration the system has been up in hours, minutes and seconds.
- **System Time** Displays the current date and time.
- **RAM Usage** Displays the RAM capacity and the available RAM memory.
- Firmware Version Displays the current firmware version of router.
- Kernel Version Displays the current kernel version of router.
- Serial Number Display the serial number of router.

Link Type WWAN1 IP Address 10.146.236.12 Netmask 255.255.255.248 Gateway 10.146.236.13 Primary DNS Server 120.80.80.80 Secondary DNS Server 221.5.88.88	Active Link Information	
IP Address 10.146.236.12 Netmask 255.255.255.248 Gateway 10.146.236.13 Primary DNS Server 120.80.80 Secondary DNS Server 221.5.88.88	Link Type	WWAN1
Netmask 255.255.255.248 Gateway 10.146.236.13 Primary DNS Server 120.80.80.80 Secondary DNS Server 221.5.88.88	IP Address	10.146.236.12
Gateway 10.146.236.13 Primary DNS Server 120.80.80 Secondary DNS Server 221.5.88.88	Netmask	255.255.258.248
Primary DNS Server 120.80.80.80 Secondary DNS Server 221.5.88.88	Gateway	10.146.236.13
Secondary DNS Server 221.5.88.88	Primary DNS Server	120.80.80
	Secondary DNS Server	221.5.88.88

Active Link Information

- Link Type Current interface for internet access.
- IP Address Displays the IP address assigned to this interface.
- Netmask

Displays the subnet mask of this interface.

- Gateway Displays the gateway of this interface. This is used for routing packets to remote networks.
- **Primary DNS Server** Displays the primary DNS server of this interface.
- Secondary DNS Server Displays the secondary DNS server of this interface.

4.2.2 Syslog

Syslog
Syslog Information
Kug ir 20.10.24 navigateworx user.err mouemt4059]. error in mouemtc, mouemtget_at_cmu_response.riz
Aug 17 20:18:24 navigateworx user.debug connection_manager[6588]: connection_manager proc_disconnected
Aug 17 20:18:24 navigateworx user. debug connection manager [6588]: cancel timer by disconnected action
Aug 17 20:18:24 navigateworx user. debug connection manager [6588]: connection of wwan1 is disconnected
Aug 17 20:18:24 navigateworx user. debug connection manager [6588]: optimal connection wan health state 0 cs 2, current connection wwan1
health state 16 cs 0
Aug 17 20:18:24 navigateworx user.warn connection manager[6588]; wwan1 is unusable
Aug 17 20:19:52 navigateworx authoriv.info webserver: pam unix(login:session): session opened for user admin by (uid=0)
Aug 17 20:19:52 navigateworx authoriv, info webserver: pam unix(login:session): session closed for user admin
Aug 17 20:20:07 navigateworx authoriv, info webserver: pam unix(login:session): session opened for user admin by (uid=0)
Aug 17 20:20:07 navigateworx authoriv, info webserver: pam unix(login:session): session closed for user admin
Aug 17 20:20:12 navigateworx authoriv, info webserver: pam unix(login:session): session opened for user admin by (uid=0)
Aug 17 20:20:12 navigateworx authoriv, info webserver: pam unix(login:session): session closed for user admin
Aug 17 21:06:02 navigateworx daemon info dnsmasg-dhcb[5060]; 181367734 available DHCP range; 192,168,5,2 192,168,5,200
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcb[5060]; 181367734 vendor class: MSFT 5.0
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcb[5060]; 181367734 client provides name: Chen
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcb[5060]: 181367734 DHCPREQUEST(1an0) 192.168.5.2 f0:76:1c:5a:4e:cc
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcb[5060]; 181367734 tags; lan0
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcb[5060]; 181367734 DHCPACK(1an0) 192.168.5.2 f0:76:1c:5a:4e:cc Chen
Aug 17 21:06:02 navigateworx daemon info dnsmaso-dhcb[5060]; 181367734 requested options; 1:netmask, 3:router, 6:dns-server, 15:domain-name.
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcb[5060]: 181367734 requested options: 31:router-discovery. 33:static-route. 43:vendor-
encab.
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcp[5060]: 181367734 requested options: 44:netbios-ns, 46:netbios-nodetype, 47:netbios-
scope,
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 requested options: 119:domain-search, 121:classless-static-route,
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcp[5060]: 181367734 requested options: 249, 252
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcp[5060]: 181367734 next server: 192.168.5.1
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 1 option: 53 message-type 5
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcp[5060]: 181367734 sent size: 4 option: 54 server-identifier 192.168.5.1
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 51 lease-time 2h
Aug 17 21:06:02 navigateworx daemon.info dnsmasg-dhcp[5060]: 181367734 sent size: 4 option: 58 T1 54m43s
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 59 T2 1h39m43s
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 1 netmask 255.255.255.0
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 28 broadcast 192.168.5.255
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 7 option: 81 FQDN 03:ff:ff:43:68:65:6e
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 6 dns-server 192.168.5.1
Aug 17 21:06:02 navigateworx daemon.info dnsmasq-dhcp[5060]: 181367734 sent size: 4 option: 3 router 192.168.5.1
Aug 17 21:09:57 navigateworx daemon.err udhcpc[6639]: sending renew
Aug 17 21:09:57 navigateworx daemon.err udhcpc[6639]: lease of 192.168.111.33 obtained, lease time 7200
Aug 17 21:09:57 navigateworx user.debug udhcpc: dhcpc update configuration of wan
Aug 17 21:09:57 navigateworx user.debug connection_manager[6588]: connection_manager proc_connected
Download Diagnosis Download Syslog Clear Refresh

Syslog Information

Download Diagnosis

Download the Diagnosis file for analysis.

Download Syslog

Download the complete syslog since last reboot.

Clear

Clear the current page syslog printing.

• Refresh

Reload the current page with latest syslog printing.

4.3 Link Management

This section shows you the setup of link management.

4.3.1 Connection Manager

Stat	tus C	Connection						
Connection Information								
Index	Туре	Status	IP Address	Netmask	Gateway			
1	WWAN1	Connected	10.146.236.12	255.255.255.248	10.146.236.13			
2	WWAN2	Disconnected						

Connection Manager->Status

• Type

Displays the connection interface

Status

Displays the connection status of this interface.

IP Address

Displays the IP Address of this interface.

Netmask

Displays the subnet mask of this interface.

• Gateway

Displays the gateway of this interface. This is used for routing packets to remote networks.

Statu	IS	Connection		
Genera	l Setting	IS		
Priority	Enab	e Connection Type	Description	
1	true	WWAN1		
2	true	WWAN2		Ø
Click Click	(±)	to add a new p to edit current i	priority interface. nterface settings.	
Click	\otimes	to delete curre	nt interface.	

Connection Manager->Connection

• Priority

Displays the priority list of default routing selection.

• Enable

Displays the connection enable status.

• **Connection Type** Displays the name of this interface.

• Description

Displays the description of this connection.

Connection Settings							
Connection Information							
Priority	1						
Enable							
Connection Type	WWAN1 •	0					
Description							
ICMP Detection Settings							
Enable							
Primary Server	8.8.8.8						
Secondary Server	114.114.114						
Interval	300	?					
Retry Interval	5	0					
Timeout	3	0					
Retry Times	3	0					
		Save Close					

Connection Settings

• Priority

Displays current index on priority list.

Connection Type

Select the available interface as outbound link. **NOTE:** specify SIM1 carrier link as WWAN1, SIM2 carrier link as WWAN2.

ICMP Detection Settings->Enable

Check this box to detect link connection status based on pings to a specified IP address.

Primary Server

Enter the primary IP address that pings will be sent to, to detect the link state. Recommend entering the IP address of known external reachable server or network (e.g. 8.8.8.8).

Secondary Server

Enter the secondary IP address that pings will be sent to, when the primary server is ping failed, router would try to ping the secondary server.

• Interval

The duration of each ICMP detection in seconds.

Retry Interval

The interval in seconds between each ping if no packets have been received.

• Timeout

Enter timeout for received ping reply to determine the ICMP detection failure.

• Retry Times

Specify the retry times for ICMP detection.

4.3.2 Cellular

Stat	us	Cellular							
Cellula	r Inform	ation							
Index	Modem	Registration	CSQ	Operator	Netwok Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	31 (-51dBm)	CHN-UNICO	DM LTE	861107038049871	460015956236598	2992	2748
				Index	1				
				Modem	EC25				
			R	egistration	Registered				
				CSQ	31 (-51dBm)				
				Operator	CHN-UNICOM				
			Ne	twok Type	LTE				
				IMEI	861107038049871				
				PLMN ID	46001				
			Local	Area Code	2508				
		Cell ID			6016C02				
	IMSI				460015956236598				
				TX Bytes	2992				
				RX Bytes	2748				
			Modem	n Firmware	EC25EFAR06A01M4G				
		Copyrigh	t © 2018 Guangzh	ou Navigatewo	orx Technologies Co. Lt	d All rights reserved			
		copyright		ou navigatewe					

NR300 Router main function is connecting to Internet by cellular modem.

Cellular->Status

Modem •

Displays the module of the modem used by this WWAN interface.

Registration •

Displays the registration status of SIM card.

CSQ •

•

Displays the signal strength of the carrier network.

- Operator Displays the wireless network provider.
- **Network Type** •

Displays the RF technology currently active. Example: LTE, UMTS, or CDMA.

IMEI •

> International Mobile Electronic Identifier. Depending on the carrier and technology used, this may be required for the carrier when activating the data contract. In some cases this will be blank.

PLMN ID

Displays the current PLMN ID, including MCC, MNC, LAC and Cell ID.

• Local Area Code

Displays the location area code of the SIM card.

Cell ID

Displays the Cell ID of the SIM card location.

IMSI

International Mobile Subscriber Identity, as read from the SIM. This is the user's network subscription.

• TX Bytes

Displays the total bytes transmitted since the time the unit was connected. NR300 router would record this data with same SIM card, reboot would not erase this data.

• RX Bytes

Displays the total bytes received since the time the unit was connected. NR300 router would record this data with same SIM card, reboot would not erase this data.

Modem Firmware

Displays firmware version of the module used by the WWAN interface.

Stat	us	<u>Cellular</u>	
Moden	n General	Settings	
Index	SIM Card	Auto APN	
1	SIM1	true	Ø
2	SIM2	true	

Cellular

SIM Card

Displays the SIM card support on this unit.

• Auto APN

Displays the Enable status of auto APN function.

SIM Card Settings	
Modem General Settings	
Index	1
SIM Card	SIM1 *
Auto APN	
Dial Number	*99#
Authentication Type	Auto 🔻
PIN Code	()
Monthly Data Limitation	0
Monthly Billing Day	1
Data Roaming	
Override Primary DNS	
Override Secondary DNS	
Modem Network Settings	
Network Type	Auto 🔻
Use All Bands	
	Save Close

SIM Card Settings

SIM Card

Displays the current SIM card settings.

Auto APN

Check this box enable auto checking the Access Point Name provided by the carrier.

- **Dial Number** Enter the dial number of the carrier.
- Authentication Type Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP.
- PIN Code

Enter a 4-8 characters PIN code to unlock the SIM.

- Monthly Data Limitation Enter the data total amount for SIM card, SIM card switchover when data reach limitation.
- Monthly Billing Day

Enter the date of renew data amount every month.

- **Data Roaming** Enable or disable the data roaming function on the router.
- **Override Primary DNS** Enter the primary DNS server will override the automatically obtained DNS.
- **Override Secondary DNS** Enter the secondary DNS server will override the automatically obtained DNS.
- Network Type Select the mode of operation of the cell module (Auto, 4G Firstly, 4G Only, etc.).
- Use All Bands

Check this box to enable all bands selection or choose specified bands.

4.3.3 Ethernet

The same instructions apply to settings for all Ethernet interfaces.

State	us F	Port Assignment	LAN	VLAN				
Ethern	et Port I	nformation						
Index	Name	Status						
1	ETH0	Up						
Interfa	ce Infor	mation						
Index	ndex Name MAC Address							
1	lan0	A8:3F:A1:E7:00:00						
DHCP I	DHCP Lease Table							
Index	MAC A	ddress IP Add	dress Le	ease Expires	Hostname			

Ethernet->Status

- Ethernet Port Information Displays the port physical connected states.
- Interface Information Displays the name and MAC address of Ethernet interface.
- DHCP Lease Table Displays the current IP address assigned to DHCP client.

Ethernet->Port Assignment

• Port

Displays the port states and numbers of this unit.

Interface

Displays the port states of belong subnet.

Port Settings					
General Settings					
Index	1				
Port	Eth0	Ψ			
Interface	LAN0	•			
			Save	Close	

Ethernet->Port Settings

• Port

Indicate the current configurate port.

• Interface

Select belong subnet for current configurate port.

Stat	us Por	t Assignment	LAN	VLAN
Gener	al Settings			
Index	Interface	IP Address	Netmask	(i)
1	LAN0	192.168.5.1	255.255.255.0	\mathbb{Z} \otimes
Multip	le IP Setting	js		
Index	Interface	IP Address	Netmask	(i)

Ethernet->LAN

• Interface

Displays current name of LAN subnet.

• IP Address Displays LAN IP address of this subnet.

Netmask

Displays subnet mask for this subnet.

LAN Settings	
General Settings	
Index	1
Interface	LAN0 V
IP Address	192.168.5.1
Netmask	255.255.255.0
MTU	1500
DHCP Settings	
Enable	
Mode	Server •
IP Pool Start	192.168.5.2
IP Pool End	192.168.5.200
Netmask	255.255.255.0
Lease Time	120
Gateway	
Primary DNS	
Secondary DNS	
WINS Server	
	Save Close
DHCP Settings	
Enable	
Mode	Relay 🔻
Relay Server	
	Save Close

Ethernet->LAN

• Interface

Select the configurate LAN port of this subnet.

IP Address

Enter LAN IP address for this interface.

• Netmask

Enter subnet mask for this subnet.

• MTU

Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.

• Enable

Check this box to enable DHCP feature on current LAN port.

• Mode

Select the DHCP working mode from "Server" or "Relay".

Relay Server

Enter the IP address of DHCP relay server.

IP Pool Start

External LAN devices connected to this unit will be assigned IP address in this range when DHCP is enabled. This is the beginning of the pool of IP addresses.

IP Pool End

This is the end of the pool of IP addresses.

Netmask

Subnet mask of the IP address obtained by DHCP clients from DHCP server.

Lease Time

The lease time of the IP address obtained by DHCP clients from DHCP server.

• Gateway

The gateway address obtained by DHCP clients from DHCP server.

• Primary DNS

Primary DNS server address obtained by DHCP clients from DHCP server.

• Secondary DNS

Secondary DNS server address obtained by DHCP clients from DHCP server.

WINS Server

Windows Internet Naming Service obtained by DHCP clients from DHCP server.

Multiple IP Settings	
General Settings	
Index	1
Interface	LAN0 V
IP Address	
Netmask	
	Save Close

Ethernet->LAN->Multiple IP Settings

Interface

Select the configurate LAN port of this subnet.

IP Address

Enter multiple IP address for this interface.

Netmask

Enter subnet mask for this subnet.

Trunk Settings	
VLAN Trunk Settings	
Index	1
Interface	LANO v
VID	10
IP Address	
Netmask	
	Save Close

Ethernet->VLAN->VLAN Trunk Settings

• Interface

- Select the LAN port for VLAN trunk.
- VID Specify the VLAN ID for VLAN trunk.
- IP Address Enter IP address for this VLAN trunk.

• Netmask

Enter subnet mask for this VLAN trunk.

4.4 Industrial Interface

The Industrial page contains tabs for making configuration settings for Serial RS232 and RS485. Select Serial from the main navigation menu to navigate to this page.

4.4.1 Serial

You could review the status of serial connection.

Stat	<u>us</u> C	onnection				
Serial 1	Serial Information					
Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status	
1	false	RS485	Transparent	TCP Client	Disconnected	
2	false	RS232	Transparent	TCP Client	Disconnected	

Serial->Status

- Enable Displays status of current serial function.
- Serial Type Displays the serial type of COM port.
- **Transmission Method** Displays the transmission method of this serial port.
- **Protocol** Displays the protocol used by this serial port.
- **Connection Status** Displays the connection status of this serial port.

Stat	us <u>(</u>	Connection							
Serial	Serial Connection Settings								
Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity			
1	false	COM1	115200	8	1	None			
2	false	COM2	115200	8	1	None			

Serial->Connection

• Enable

Displays status of current serial function.

• Port

Displays the serial type of COM port.

Baud Rate

Displays the serial port baud rate.

- Data Bits Displays the serial port Data Bits.
- Stop Bits

Displays the serial port Stop Bits.

• Parity

Displays the serial port parity.

Connection Settings						
Serial Connection Settings						
Index	1]				
Enable						
Port	COM1 •]				
Baud Rate	115200 •]				
Data Bits	8 •]				
Stop Bits	1 •]				
Parity	None •]				
Transmission Settings						
Transmission Method	Transparent •]				
MTU	1024	0				
Protocol	TCP Client •]				
Remote IP Address]				
Remote Port	2000]				
		Save Close				

Serial->Connection Settings

Baud Rate

Select the serial port baud rate. Supported values are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.

• Data Bits

Select the values from 7 or 8.

Stop Bits

Select the values from 1 or 2.

• Parity

Select values from none, even, odd.

Transmission Method

Select the transmission method for serial port. Optional for "Transparent", "Modbus RTU Gateway" and "Modbus ASCII Gateway".

MTU

Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.

Protocol

Select the mode for Serial IP communication. Supported modes are UDP, TCP Server, or TCP Client.

Remote IP Address

Enter the IP address of the remote server.

Remote Port

Enter the port number of the remote server.

Below window displays different settings when you select **TCP Server** on Protocol.

Transmission Settings					
Transmission Method	Transparent •				
MTU	1024 ⑦				
Protocol	TCP Server				
Local IP Address					
Local Port	2000				

Serial->Connection Settings

Local IP Address

Enter the IP Address of the local endpoint.

Local Port

The port number assigned to the serial IP port on which communications will take place.

Below window displays different settings when you select **UDP** on Protocol.

Transmission Settings					
Transmission Method	Transparent 🔹				
MTU	1024 ⑦				
Protocol	UDP v				
Local IP Address					
Local Port	2000				
Remote IP Address					
Remote Port	2000				

Serial->Connection Settings

Local IP Address

Enter the IP Address of the local endpoint.

- Local Port The port number assigned to the serial IP port on which communications will take place.
- **Remote IP Address** Enter the IP address of the remote server.
- **Remote Port** Enter the port number of the remote server.

4.5 Network

4.5.1 Firewall

Firewall rules are security rule-sets to implement control over users, applications or network objects in an organization. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement.

ACL	Port Mapping	g DMZ						
General Set	ttings							
			Default Policy	Accept	*			
ACL rule Se	ettings							
Index	Description	Protocol	Source Address	Source Port	Destination Address	Destination Port		(\div)
Firewall	Firewall->ACI							

• Default Policy

Select the "Accept" or "Drop" from the list, the packets which are not included in the access control list will be processed by the default filter policy.

An access control list (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

ACL Settings	
General Settings	
Index	1
Description	
Protocol	All
Source Address	
Destination Address	Ø
	Save Close

Firewall->ACL

• Description

Add a description for this rule.

Protocol

All: Any protocol number. TCP: The TCP protocol. UDP: The UDP protocol. TCP & DUP: both TCP and UDP protocol ICMP: The ICMP protocol.

Source Address

A specific host IP address can also be specified, or a range of IP addresses via a bitmask (the box following the /).

Destination Address

A specific IP address can also be specified, or a range of IP addresses via a bitmask (the box following the /).

Port Mapping Settings	
Port Mapping rule Settings	
Index	1
Description	
Protocol	All v
Remote Address	
Remote Port	
Local Address	
Local Port	
	Save Close

Firewall->Port Mapping

• Description

Add a description for this rule.

Protocol

All: Any protocol number. TCP: The TCP protocol. UDP: The UDP protocol.

Remote Address

Enter a WAN IP address that is allowed to access the unit.

Remote Port

Enter the external port number range for incoming requests.

Local Address

Sets the LAN address of a device connected to one of the Fusion's LAN interfaces. Inbound requests will be forwarded to this IP address.

Local Port

Sets the LAN port number range used when forwarding to the destination IP address.

ACL	Port Mapping	DMZ	
General Setting	s		
		Enable	
		Remote Address	0.0.0.0/0 ⑦
		DMZ Host Address	

Firewall->DMZ

• Enable

Check this box to enable DMZ function.

Remote Address

Optionally restricts DMZ access to only the specified WAN IP address. **NOTE:** If set to 0.0.0.0/0, the DMZ is open to all incoming WAN IP addresses.

• DMZ Host Address

The WAN IP address which has all ports exposed except ports defined in the Port Forwarding configuration.

1-1 NAT Settings	
1-1 NAT Settings	
Index	1
Description	
Interface Address	
Host Address	
Interface To Host	
	Save Close

Firewall->NAT

- **Description** Enter a description of 1-to-1 NAT setting.
- Interface Address
 Specify the interface address that need to be accessed before NAT.
- Host Address
 Specify the host address that need to be accessed after NAT.
- Interface To Address Specify the interface that connected to host, like lan0, lan1, lan2, lan3.

4.5.2 Route

Static Routing refers to a manual method of setting up routing between networks. Select the Static Routing tab to add static routes to the Static Route Table.

Please refer current route table as below.

Statu	is Static Ro	oute									
Route Table Information											
Index	Destination	Netmask	Gateway	Metric	Interface						
1	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0						
Route	->Route Tc	able Informati	on								

Destination

Displays the destination of routing traffic.

Netmask

Displays the subnet mask of this routing.

• Gateway

Displays the gateway of this interface. This is used for routing packets to remote networks.

Metric

Displays the metric value of this interface.

• Interface

Displays the outbound interface of this route.

Static Route Settings			
Route Table Information			
Index	1		
Description			
IP Address			
Netmask			
Gateway			
Interface		0	
		Save	Close

Route->Static Route Settings

• Description

Enter the description of current static route rule.

IP Address

Enter the IP address of the destination network.

- **Netmask** Enter the subnet mask of the destination network.
- Gateway
 Enter the IP address of the local gateway.
 - Interface

Please refer to the Network->Route->Status interface.

4.5.3 IP Passthrough

IP Passthrough mode, disables NAT and routing and passes the WAN IP address from the WAN interface to the device connected on the local Interface. It is used instead of Network Address Translation (NAT) in order to make the router "transparent" in the communication process.

IP Passthrough	
General Settings	
Enable	
Passthrough Host MAC	
Remote HTTPS Access Reserved	
Remote Telnet Access Reserved	
Remote SSH Access Reserved	

Network->IP Passthrough

- Enable Check this box will enable IP Passthrough.
- Passthrough Host MAC
 - Enter the MAC of passthrough host to receive the WAN IP address.
- **Remote HTTPS Access Reserved** Check this box to allow to remote access the router via https while enable IP Passthrough mode.
- **Remote Telnet Access Reserved** Check this box to allow to remote telnet to the router while enable IP Passthrough mode.
- **Remote SSH Access Reserved** Check this box to allow to remote SSH to the router while enable IP Passthrough mode.

4.6 Applications

4.6.1 DDNS

DDNS is a system that allows the domain name data of a computer with a varying (dynamic) IP addresses held in a name server to be updated in real time in order to make it possible to establish connections to that machine without the need to track the actual IP addresses at all times. A number of providers offer Dynamic DNS services (DDNS), free or for a charge.

You could review the status of DDNS as below.

<u>Status</u>	DDNS		
DDNS Status			
		Status	Updating
		Public IP Address	
Status	DDNS		
General Setting	js		
		Enable	
		Keep Updating	
		DDNS Provider	no-ip •
		Enable SSL	
		Username	
		Password	
		Hostname	
		Log Level	Error •

DDNS

- Enable Check this box to enable the DDNS service.
- Keep Updating

Check this box to keep updating the IP address to the DDNS server.

• DDNS Provider

Select the DDNS provider from the list, options from "DynDNS", "no-ip", "3322" and custom.

DDNS Server

The internet address to communicate the Dynamic DNS information to. This option is available after you select **custom** on DDNS Provider.

DDNS Path

DDNS path for custom type.

Check IP Server
 Check IP Server for custom type

- Check IP Path Check IP Path for custom type.
- Enable SSL Enable SSL for connection.
- Username Enter the user name used when setting up the account. Used to login to the Dynamic DNS service.
 Password

Enter the password associated with the account.

- Hostname Enter the hostname associated with the account.
 - **Log Level** Select the log output level from "none", "Debug", "Notice", "Info" and "Error".

4.6.2 SMS

•

SMS allows user to send the SMS to control the router or get the running status of the router.

<u>5M5</u>	
General Settings	
Enable	
Authentication Type	Password •
Allow Phone Book	
Index Description Phone Number	\oplus
Phone Number Settings	
Allow Phone Book	
Index	1
Description	
Phone Number	
	Save Close
Application->SMS	

• Enable

Check this box to enable SMS feature.

- Authentication Type Specify the authentication mode for SMS, optional for "None" and "Password".
- Description
 Enter the description of the Phone Book
- **Phone Number** Enter the special phone number and only allow this phone number to send SMS to the router

4.6.3 Schedule Reboot

Schedule reboot allows user to define the time for router reboot itself.

Schedule Reboot	
General Settings	
Enable	
Time to Reboot	00:00 ⑦
Day to Reboot	0 ⑦

Application->Schedule Reboot

• Enable

Check this box to enable schedule reboot feature.

- **Time to Reboot** Enter the time of each day to reboot device. Format: HH(00-23):MM(00-59).
- **Day to Reboot** Enter the day of each month to reboot device. 0 means every day.

4.7 VPN

4.7.1 OpenVPN

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability.

You could review all OpenVPN connection as below.

Sta	atus	OpenVPN X.509 Certificate							
OpenVPN Information									
Index	Enable	Description	Status	Uptime	Virtual IP				

VPN->OpenVPN->Status

- Enable Displays current OpenVPN settings is enable or disable.
- Status Displays the current VPN connection status.
- **Uptime** Displays the connection time since VPN is established.
- Virtual IP

Displays the virtual IP address obtain from remote side.

OpenVPN Settings	
General Settings	·
Index	1
Enable	
Description	
Mode	Client •
Protocol	UDP •
Connection Type	TUN •
Server Address	
Server Port	1194
Authentication Method	X.509 • ⑦
Encryption Type	BF-CBC •
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	0 ⑦
Private Key Password	
Output Verbosity Level	3
Advanced Settings	
Enable NAT	· ·

VPN->OpenVPN

- Enable Check this box to enable OpenVPN tunnel.
- **Description** Enter a description for this OpenVPN tunnel.
- Mode Select from "Client" or "P2P".
- Protocol

Select from "UDP" or "TCP Client".

Connection Type

Select from "TUN", "TAP" which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.

Server Address

Enter the IP address or domain of remote server.

• Server Port

Enter the negotiate port on OpenVPN server.

Authentication Method

Select from "X.509", "Pre-shared", "Password", and "X.509 And Password".

• Encryption Type

Select from "BF-CBC", "DES-CBC", "DES-EDE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".

Username

Enter the username for authentication when selection from "Password" or "X.509 And Password".

Password

Enter the password for authentication when selection from "Password" or "X.509 And Password".

Local IP Address

Enter the local virtual IP address when select "P2P" mode.

Remote IP Address

Enter the remote virtual IP address when select "P2P" mode.

Local Netmask

Enter the local netmask when select "TAP" connection type.

TAP Bridge

Select the specified LAN that bridge with OpenVPN tunnel when select "TAP" connection type.

- **Renegotiate Interval** Enter the renegotiate interval if connection is failed.
- Keepalive Interval

Enter the keepalive interval to check the tunnel is active or not.

Keepalive Timeout

Enter the keepalive timeout, once connection is failed it will trigger the OpenVPN reconnect.

- **Fragment** Enter the fragment size, 0 means disable.
- **Private Key Password** Enter the private key password for authentication when selection from "X.509" or "X.509 And Password".
- **Output Verbosity Level** Enter the level of the output log and values.

Advanced Settings	
Enable NAT	
Enable PKCS#12	
Enable X.509 Attribute nsCertType	
Enable HMAC Firewall	
Enable Compression LZ0	
Additional Configurations	Ø
	Save Close

VPN->OpenVPN->Advanced Settings

• Enable NAT

Check this box to enable NAT, the source IP of host behind router will be disguised before accessing the remote end.

• Enable PKCS#12

It is an exchange of digital certificate encryption standard, used to describe personal identity information.

- Enable X.509 Attribute nsCertType Require that peer certificate was signed with an explicit nsCertType designation of "server".
- Enable HMAC Firewall Add additional layer of HMAC authentication on the top of the TLS control channel to protect against DoS attacks.
- Enable Compression LZO Compress the data.
- Additional Configurations Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.

Status	OpenVPN	N <u>X.509 C</u>	ertificate							
X.509 Ce	rtificate Import									
			Connection Index	1	•	·]				
			CA Certificate	Choose File	No file chosen		٢			
			Local Certificate File	Choose File	No file chosen		٢			
			Local Private Key	Choose File	No file chosen		٢			
			HMAC firewall Key	Choose File	No file chosen	1	٢			
			Pre-shared Key	Choose File	No file chosen		٢			
			PKCS#12 Certificate	Choose File	No file chosen		٢			
X.509 Ce	rtificate Files									
Index	File Name F	File Size	Date Modified							

VPN->OpenVPN->X.509 Certificate

- Connection Index
 Displays the current connection index for OpenVPN channel.
- CA Certificate Import CA certificate file.
- Local Certificate File
 Import Local Certificate file.
- Local Private Key Import Local Private Key file.
- HMAC Firewall Key
 Import HMAC Firewall Key file.
- **Pre-shared Key** Import the pre-shared key file.
- PKCS#12 Certificate
 Import PKCS#12 Certificate

4.7.2 IPSec

IPSec facilitates configuration of secured communication tunnels. The various tunnel configurations will be displayed in the Tunnel Table at the bottom of the page. All tunnels are create using the ESP (Encapsulating Security Payload) protocol.

State	us	IPSec			
IPSec 1	Informati	on			
Index	Enable	Description	Status	Uptime	
VPN-	>IPSec	:->Status			

• Enable

Displays current IPSec settings is enable or disable.

• Description

Displays the description of current VPN channel.

• Status

Displays the current VPN connection status.

• Uptime

Displays the connection time since VPN is established.

IPSec Settings	
General Settings	
Index	1
Enable	
Description	
Remote Gateway	
IKE Version	IKEv1 •
Connection Type	Tunnel 🔹
Negotiation Mode	Main 🔹
Authentication Method	Pre-shared Key and Xauth 🔻
Local Subnet	
Local Pre-shared Key	
Local ID Type	IPv4 Address
Xauth Identity	
Xauth Password	
Remote Subnet	
Remote ID Type	IPv4 Address 🔹

VPN->IPSec

• Enable

Select Enable will launch the IPSec process.

Description

Enter a description for this IPSec VPN tunnel.

Remote Gateway

Enter the IP address of the remote endpoint of the tunnel.

IKE Version

Internet Key Exchange, select from "IKEv1" or "IKEv2".

• Connection Type

Select from "Tunnel" or "Transport". Tunnel: In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications.

Transport: In transport mode, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted.

Negotiation Mode

Select from "Main" or "Aggressive".

Authentication Method

Select from "Pre-shared Key" or "Pre-shared Key and Xauth".

Local Subnet

Ener the IP address with mask if a network beyond the local LAN will be sending packets through the tunnel.

NOTE: The Remote subnet and Local subnet addresses must not overlap!

Local Pre-shared Key

Enter the pre-shared key which match the remote endpoint.

Local ID Type

The local endpoint's identification. The identifier can be a host name or an IP address.

Xauth Identity

Enter Xauth identity after "Pre-shared Key and Xauth" on authentication Method is enabled.

Xauth Password

Enter Xauth password "Pre-shared Key and Xauth" on authentication Method is enabled.

Remote Subnet

Enter an IP address with mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address. **NOTE:** The Remote subnet and Local subnet addresses must not overlap!

Remote ID Type

The authentication address of the remote endpoint.

IKE Proposal Settings		
Encryption algorithm	AES-256	T
Hash Algorithm	SHA2 256	T
Diffie-Hellman group	Group5(modp1536)	T
Lifetime	1440	
ESP Proposal Settings		
Encryption algorithm	AES-256	T
Hash Algorithm	SHA2 256	•
Diffie-Hellman group	Group5(modp1536)	v
Lifetime	60	
Advanced Settings		
DPD Interval	30	0
DPD Timeout	90	0
Additional Configurations		0
		Save Close

VPN->IPSec

- Encryption Algorithm (IKE)
 Select 3DES AES-128, AES-192, or AES-256 encryption.
- Hash Algorithm (IKE)
 Select from MD5, SHA1, SHA2 256, SHA2 384 or SHA2 512 hashing.
- Diffie-Hellman Group (IKE)
 Negotiate (None) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) etc.
- Lifetime (IKE) How long the keying channel of a connection should last before being renegotiated.
- Encryption Algorithm (ESP) Select 3DES AES-128, AES-192, or AES-256 encryption.
- Hash Algorithm (ESP) Select from MD5, SHA1, SHA2 256, SHA2 384 or SHA2 512 hashing.
- Diffie-Hellman Group (ESP)
 Negotiate (None) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) etc.
- Lifetime (ESP) How long a particular instance of a connection should last, from successful negotiation to expiry.
- **DPD Interval** Enter the interval after which DPD is triggered if no IPsec protected packets is received from the peer.
- **DPD Timeout** Enter the remote peer probe response timer.
- Additional Configurations Enter some other options of IPSec in this field. Each expression can be separated by a ';'.

4.7.3 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message could be transmitted and encapsulation and decapsulation could be realized at both ends.

Stat	us	GRE					
GRE In	formation						
Index	Enable	Description	Mode	Status			

VPN->GRE->Status

• Enable

Displays current GRE settings is enable or disable.

- **Description** Displays the description of current VPN channel.
- Mode

Displays the current VPN mode.

Status

Displays the current VPN connection status.

GRE Settings	
GRE Information	
Index	1
Enable	
Description	
Mode	Layer 3 🔹
Remote Gateway	
Local Virtual IP	
Local Virtual Netmask	255.255.255.252
Tunnel key	()
Enable NAT	
	Save Close

VPN->GRE

- Enable Check this box to enable GRE.
- **Description** Enter the description of current VPN channel.
- Mode

Specify the running mode of GRE, optional are "Layer 2" and "Layer 3".

- **Remote Gateway** Enter the remote IP address of peer GRE tunnel.
- Local Virtual IP
 Enter the local tunnel IP address of GRE tunnel.
- Local Virtual Netmask Enter the local virtual netmask of GRE tunnel.
- **Tunnel Key** Enter the authentication key of GRE tunnel.
- Enable NAT Check this box to enable NAT function.
- **Bridge Interface** Specify the bridge interface work with Layer 2 mode.

4.8 Maintenance

4.8.1 Upgrade

When newer versions of NR300 firmware become available, the user can manually update the unit by uploading a package to the unit.

NOTE: The unit need manually reboots once the upload completes, thus taking the NR300 router out of service during approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.

CAUTION: It is important to have a stable power source and ensure that power to the Fusion is not interrupted during a firmware upgrade.

Firmware			
Firmware Upgrade			
	Firmware	Choose File No file chosen] 🕹

4.8.2 Software

When release a new feature (APP Package) of NR300 router, the user can manually install to the unit by uploading a package. Or user can uninstall this feature (APP Package) from router.

NOTE: The unit need manually reboots once the upload/uninstall completes, thus taking the NR300 router out of service during approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.

Softw	/are			
Softwa	are Install			
		Software	Choose File No file chosen	≎
Softwa	are List			
Index	Name	Version	Installed Time	
1	dmvpn	1.0.0-2	Fri May 31 18:47:08 2019	\otimes
Click	to upload the	APP Package		
Click	⊗ to delete the <i>i</i>	APP Package.		

Note: We are working different kinds of the APP Packages. Please contact us to get them in case of you would like to test.

4.8.3 System

This section allows you to review the device system settings.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security	
General Setti	ngs						
			Hostname	navigateworx.rout	er		
			User LED Type	None	•		
Time Zone Se	ettings						
			Time Zone	UTC+08:00	•		
		Custo	mized Time Zone			0	
Time Synchro	onisation						
			Enable				
		Pr	imary NTP Server	pool.ntp.org			
		Seco	ndary NTP Server	1.pool.ntp.org			
-							

System->General

Hostname

User-defined router name, which might be use for IPSec local ID identify.

- User LED Type Defined the User LED behavior.
- Time Zone

Select the zone where the device is in use.

Customized Time Zone

Customized the zone where the device is in use.

Enable (NTP Client)

Selected Enabled to utilize the NTP client to synchronize the device clock over the network using a time server (NTP server).

Primary NTP Server

Enter the IP address (or host name) of the primary time server.

Secondary NTP Server

Enter the IP address (or host name) of the secondary time server.

Gener	ral <u>Acc</u>	counts	Syslog	Web Server	Telnet	SSH	Security		
Account	t Settings								
				Administrator	admin				
				Old Password					
				New Password					
			Co	onfirm Password					
Visitor 9	Settings								
Index	Username	Password							(e)

System->Account

Administrator

Displays the name of current administrator, default as "admin".

- Old Password Enter the old password of administrator.
- **New Password** Enter the new password of administrator.
- **Confirm Password** Confirm the new password of administrator.

Account Settings				
	Index	1		
	Username			
	Password			
			Save	Close

Username

Enter a username of visitor privilege

Password

Enter the new password of current visitor account.

Syslog displays system logs that are stored in the log buffers.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security	
General Setti	ngs						
			Log Location	RAM	•		
			Log Level	Debug	•		
Remote Syste	og Settings						
		Enab	le Remote Syslog				
		Remo	ote Syslog Server				
		Re	mote Syslog Port	514			

System->Syslog

- Log Location Select the log store location to "RAM".
- Log Level Select the log output level from "Debug", "Notice", "Info", "Warning" or "Error".
- Enable Remote Syslog Check this box to enable remote syslog connection.

• **Remote Syslog Server** Enter the IP address of remote syslog server.

Remote Syslog Port

Enter the port for remote syslog server listening.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security	
General Setti	ings						
			HTTP Port	80			
			HTTPS Port	443			
Certificate Se	ettings						
			Private Key	Choose File N	lo file chosen	ۍ	
			Certificate File	Choose File N	lo file chosen	ۍ 🔁	

System->Web Server

HTTP Port

Enter the port for Hypertext Transfer Protocol. A well-known port for HTTP is port 80.

HTTPS Port

Enter the port for HTTPS Protocol. A well-known port for HTTPS is port 443.

• Private Key

Import private Key file for HTTPS connection.

Certificate File

Import certificate file for HTTPS connection.

General	Accounts	Syslog	Web Server	<u>Telnet</u>	SSH	Security
General Settings						
			Telnet Port	23		
System->	System->Telnet					

• Telnet Port

Enter the port for telnet access. A well-known port for HTTP is port 23.

General	Accounts	Syslog	Web Server	Telnet	<u>SSH</u>	Security		
General Settings								
			SSH Port	22				
		Allow Passwo	rd Authentication					
			Public Key					

System->SSH

SSH Port

Enter the port for SSH access. A well-known port for HTTP is port 22.

• Allow Password Authentication Check this box to enable SSH authentication.

• Public Key

Enter the public Key SSH authentication.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security	
Remote Access Settings							
		Rem	ote HTTP Access				
		Remo	te HTTPS Access				
		Remo	te Telnet Access				
		Rer	note SSH Access				
DDoS Defens	es Settings						
			DDoS Defenses				

System->Security

Remote HTTP Access

Check this box to allow remote HTTP access.

Remote HTTPS Access
 Check this box to allow remote HTTPS access.

• Remote Telnet Access

Check this box to allow remote Telnet access.

Remote SSH Access Check this box to allow remote SSH access.

• DDoS Defenses

Check this box to enable DDoS defenses

4.8.4 Configuration

The Unit Configuration tab allows you to save parameters (settings in the Web interface) to a file. Conversely, if you have saved settings from the NR300 router to a file, you can Import these previously-saved configuration settings to the NR300 router as well.

<u>Configuration</u>	
Configuration Management	
Factory settings	Restore
Configuration File Download	Download
Configuration File Upload	Choose File No file chosen

System->Configuration

Restore

Reset the unit to factory default settings.

- **Download** Download the configuration file from NR300 router.
- Configuration File Upload
 Import previously-saved configuration file.

4.8.5 Debug Tools

Ping	Traceroute	AT Debug	
Ping Settings			
		Host Address	
		Ping Count	5
		Local IP Address	
Debug To	ols->Ping		

Host Address

Enter a host IP address or domain name for ping.

Ping Count

Enter the ping times.

• Local IP Address

Enter the ping source IP address or leave it blank.

Ping	Traceroute	AT Debug			
Traceroute S	Traceroute Settings				
			Host Address		
			Max Hops	30	
Debug Tools->Traceroute					

Host Address

Enter a host IP address or domain name for traceroute.

• Max Hops

Enter the max hops for traceroute.

Ping	Traceroute	AT Debug			
AT Debug Settings					
			AT Command		
Debug T	ools->AT De	ebug			

• AT Command

Enter the AT command of the module.

Appendix A - Glossary

APN:	Access Point Name
GPRS:	General Packet Radio Service
HSPA:	High Speed Packet Access
HSDPA:	High-Speed Downlink Packet Access
HSUPA:	High-Speed Uplink Packet Access
LTE:	3GPP Long Term Evolution
IMEI:	International Mobile Equipment Identity
ICCID:	Integrated Circuit Card Identifier
PIN:	Personal Identification Number
PPP:	Point-to-Point Protocol
RSSI:	Received Signal Strength Indication
SIM:	Subscriber Identity Module
SMS:	Short Message Service
DHCP:	Dynamic Host Configuration Protocol
LAN:	Local Area Network
LED:	Light-Emitting Diode
NTP:	Network Time Protocol
SMA:	SubMiniature version A (connector)
SSID:	Service Set Identifier
TCP/IP:	Transmission Control Protocol / Internet Protocol
UDP:	User Datagram Protocol
VPN:	Virtual Private Network
VDC:	Voltage, Direct Current

Appendix B -Q&A

No Signal

Phenomenon

NR300 Router modem status show no signal.

Possible Reason

- Antenna installation is wrong.
- Modem failure.

Solution

- Check the LTE antenna or replace with new one.
- Check the cellular page confirm modem is detected correctly or not.

Cannot detect SIM card

Phenomenon

NR300 Router cannot detect SIM card, cellular is not failed to connect to base station.

Possible Reason

- SIM card damage.
- SIM bad contact.

Solution

- Replace SIM card.
- Re-install SIM card.

Poor Signal

Phenomenon

NR300 Router no signal or poor signal.

Possible Reason

- Antenna installation is wrong.
- Area signal weak.

Solution

- Check the antenna and re-connect it.
- Contact Telecom Operator to confirm signal problem.
- Change to high-gain antenna.

IPSec VPN established, but LAN to LAN cannot communicate

Phenomenon

IPSec VPN established, but LAN to LAN cannot communicate

Possible Reason

- Both subnets are not match the interested traffic.
- IPSec second phase (ESP) settings is not match.

Solution

- Check the both subnet settings.
- Check IPSec second phase (ESP) setting.

Forget Router Password

Phenomenon

Forget router login password.

Possible Reason

User has changed the password.

Solution

After router power on, press RESET button between 3 to 10 seconds then release, router need manually reboot and reset to factory default settings (Username/Password is admin/admin).

Appendix D - CLI

Command-line interface (CLI) is a software interface that provide another configurable way to set parameters on our router. We could use Telnet or SSH connect to our router for CLI input.

NR300 CLI Access

navigateworx.router login: admin

Password: admin

>

CLI reference commands

>?

config	Change to the configuration mode
exit	Exit this CLI session
help	Display an overview of the CLI syntax
ping	Ping
reboot	Reboot system
show	Show running configuration or running status
telnet	Telnet Client
traceroute	TraceRoute
upgrade	Upgrade firmware
version	Show firmware version
a	

e.g.

>

> version 1.0.0 (337913f)

> ping www.baidu.com

PING www.baidu.com (14.215.177.38): 56 data bytes 64 bytes from 14.215.177.38: seq=0 ttl=54 time=10.826 ms 64 bytes from 14.215.177.38: seq=1 ttl=54 time=10.284 ms 64 bytes from 14.215.177.38: seq=2 ttl=54 time=10.073 ms 64 bytes from 14.215.177.38: seq=3 ttl=54 time=10.031 ms 64 bytes from 14.215.177.38: seq=4 ttl=54 time=10.347 ms

--- www.baidu.com ping statistics ---

5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 10.031/10.312/10.826 ms.

How to Configure the CLI

CONTEXT SENSITIVE HELP

[?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.

AUTO-COMPLETION

The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained.

[space] - Auto-completes, or if the command is already resolved inserts a space.

MOVEMENT KEYS

[CTRL-A] - Move to the start of the line

- [CTRL-E] Move to the end of the line.
- [up] Move to the previous command line held in history.
- [down] Move to the next command line held in history.
- [left] Move the insertion point left one character.
- [right] Move the insertion point right one character.

DELETION KEYS

- [CTRL-C] Delete and abort the current line
- [CTRL-D] Delete the character to the right on the insertion point.
- [CTRL-K] Delete all the characters to the right of the insertion point.
- [CTRL-U] Delete the whole line.

[backspace] - Delete the character to the left of the insertion point.

ESCAPE SEQUENCES

- !! Subsitute the the last command line.
- IN Substitute the Nth command line (absolute as per 'history' command)
- I-N Substitute the command line entered N lines before (relative)